ABSTRACT

In an anti-virus scanning system for computer files being transferred between computers, the number of files requiring detailed scanning is first reduced by identifying files which are instances of programs which are known and deemed to be safe. This is done by reference to a database of known executables which records characteristics which can be used as the basis for identifying a file as an unchanged instance of a known executable. Secondly, these characteristics can then also be used to identify files which are changed instances of known executables. These are extremely suspicious, since the most likely cause of change is infection by a file infecting virus, so these files are classed as likely to be malware.